無線ＬＡＮによるモバイルコンピューティングの実現方式の検討

久埜　豊†　　市川　武男†　　飯塚　正孝†　　守倉　正博†

現在，米国のIEEE 802.11 ワーキンググループにおいて標準化が進められている５ＧＨｚ帯高速無線ＬＡＮを用いたモバイルコンピューティングの実現方式の検討結果について報告する．本報告で扱う無線ＬＡＮの特徴は，モバイルコンピューティングを行う際の必須の機能である，Ｖｉｒｔｕａｌ　ＬＡＮ機能(ＡＬＡＮ)，公開鍵認証機能を有する点にある．

本報告では，上記の特徴により，次の２点を実現していることについて述べる．

①出先のネットワークでのセキュリティ確保が容易となる

②出先のネットワークでのマルチキャストを用いたアプリケーションがネットワークの設定を変更せずに可能である

また，無線ＬＡＮの将来的な利用形態について検討した結果についても報告する．

Implementation Scheme of Mobile Computing System by Wireless LAN

In this report, 5GHz High bit rate Wireless LAN based on IEEE 802.11 standard is introduced. This system has two main merit for mobile computing, ie,

(1) it adopts public key authentification

(2) it provides Virtual LAN function, ALAN.

From the Above two merits,

(1) This system secure terminals in foreign networks they move into.

(2) provides multicast applications without any network setting of terminals.

Future usage for the proposed wireless LAN is also described.

１．はじめに

本報告では，５ＧＨｚ帯高速無線ＬＡＮを用いたモバイルコンピューティングの実現方式の検討結果について述べる．提案するシステムの特徴は，無線ＬＡＮを用いてモバイルコンピューティングを行う際の必須の機能である，Ｖｉｒｔｕａｌ　ＬＡＮ機能(ＡＬＡＮ)，公開鍵認証機能を実装している点である．そこで，以下では，この両機能を中心に紹介し，本システムの特徴を活かしたモバイルコンピューティングのアプリケーションについて検討した結果に触れる．

近年，ＰＩＡＦＳ，ＤＯＰＡ，Ｉ－ｍｏｄｅなどの登場により，無線によるモバイルコンピューティングの環境が急速に整ってきた．今後もこの流れは加速され，マルチメディア・コンテンツの拡充も相俟って，モバイル環境における高速伝送に対する需要は拡大し続けると考えられる．

上記の需要に応える得る無線インフラとしては，現在ＩＥＥＥ８０２．１１において標準化活動が最終段階に入った５ＧＨｚ帯無線ＬＡＮが有力である．本方式は，

①装置の小型化・低価格化が可能である

②標準化されているため，相互接続性に優れており，異なる職場へ無線ＬＡＮ端末を持ちこんで使用することが可能である．

③Ethernet ベースであるため，上位レイヤへのインパクトがない

と，モバイルコンピューティングに不可欠な点をクリアしている．

本報告で対象とするシステムは

ＩＥＥＥ８０２．１１標準規格の利点を最大限に生かして職場の外部のネットワークにおけるモバイルコンピューティングを実現するために、以下の２つの特徴を有す

†ＮＴＴ　アクセスサービスシステム研究所
NTT Access Network Service Systems Laboratories

る。
①出先のネットワークでのセキュリティ確保が容易となる，公開鍵認証を採用
②バーチャルＬＡＮシステム(ロジカルオフィス ｳﾞ)との結合を行うため，レイヤ２とレイヤ３の中間にミドルウェア(ＡＬＡＮ層)を定義
上記の２特徴によって，基本的なモバイルコンピューティングを行うことが可能となる．

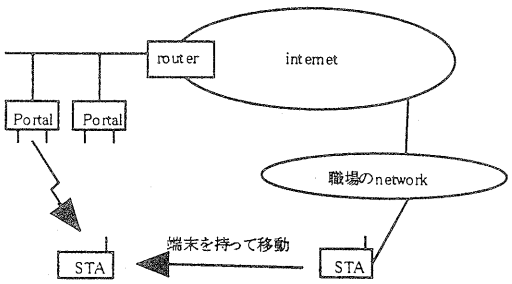
また，将来的な本システムの応用として，
①教育用自習プログラム，医療分野など
②会議室などの公共／準公共的なスペースでの利用
③ＯＣＮなどの公衆網や，他の企業のＬＡＮからのアクセス
が考えられる．これらを実現するためには，
・会議室を予約したユーザ，問題を回答した学習者だけがアクセスできるようにするなど，接続条件の柔軟な設定ができること
・ネットワーク外部からファイヤーウォールを通りぬけて職場のネットワークにアクセスすることができること
が必要である．

本報告では，まず，対象とする５ＧＨｚ帯高速無線ＬＡＮシステムの特徴を紹介する．ついで，本システムの主要な拡張機能である，公開鍵認証機能と，バーチャルＬＡＮ機能について，詳細な説明を行う．さらに，無線ＬＡＮの高度な利用方法の提案と，その実現のために必須な機能について検討した結果を報告する．

１．提案する高速無線ＬＡＮシステムの概要

前述のように，５ＧＨｚ帯は，装置の小型化，低価格化と，データの高速伝送が両立できる周波数帯であることから，モバイルコンピューティングへの応用が期待されている．

第１図に，システムの構成図を示す．Ethernet のＬＡＮに接続するＰｏｒｔａｌと，ユーザが持ち運ぶ無線端末ＳＴＡの間が無線で伝送される区間である



第１図　高速無線ＬＡＮシステム

(第２図に示すプロトコル構成図参照)．無線区間のＭＡＣ層が，ネットワーク層以上からは Ethernet に見えているため，従来のアプリケーションをそのまま使用することができる．

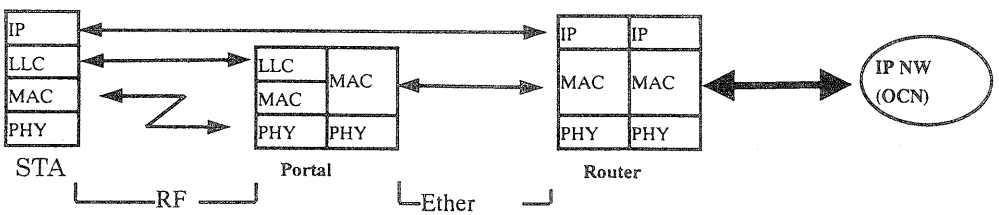
無線を用いたモバイルコンピューティングでは，セキュリティ機能(認証，暗号化)，位置登録機能(帰属管理機能)は必須である．これらの機能についての，本システムのベースとなった IEEE802..11 では，以下のような規定となっている。

①　セキュリティ
接続を行うＰｏｒｔａｌとＳＴＡは，認証鍵，暗号化鍵を事前に共有していなければならないと規定されている．
このように規定されているために，広範囲かつ自由に移動するユーザが，接続を行う場合には適していない．

②　位置管理機能
接続するＰｏｒｔａｌが位置(帰属)管理を行ってＳＴＡまでパケットの配送を行うことが規定されている．

しかし，職場にいたときと同じ，ＩＰアドレス，ＭＡＣアドレスを外部のネットワークでは使用する方法が規定されていないため外部のネットワークで，ホームネットワークに接続しているときと同様にマルチキャストを用いたアプリケーションを利用したいユーザのためには，Ethernet のパケットを外部にカプセリングして転送する機能を追加する必要がある．

上記の為に，本システムでは以下に述べる機能拡張を実現している．



第２図　本システムのプロトコルスタック

3．公開鍵認証，公開鍵配送について

3－1本システムにおいて採用されている公開鍵認証と公開鍵配送の概要

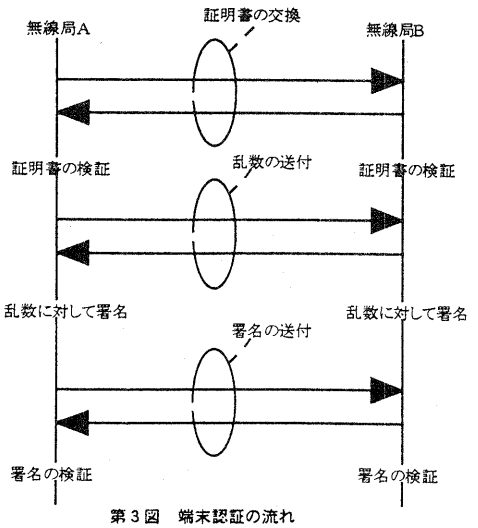
3－1－1．公開鍵認証

公開鍵認証とは，公開鍵暗号を用いることにより，認証情報データベースにアクセスせずに通信相手の認証を行う方法である．

公開鍵暗号では，ある情報Ｉが秘密鍵ＳＫを用いて暗号化された(＝Ｅ(ＳＫ，Ｉ)を算出した)かどうかを，公開鍵ＰＫを用いて復号する(すなわちＦ(ＰＫ，Ｅ(ＳＫ，Ｉ))を算出する)ことにより検証できる．(最も有名なＲＳＡ暗号の場合は，Ｉ＝Ｆ(ＰＫ，Ｅ(ＳＫ，Ｉ)が成り立つ．)秘密鍵で暗号化された情報(上の手順におけるＥ(ＳＫ，Ｉ)を署名と呼び，ＩとＥ(ＳＫ，Ｉ)の組のことを証明書と呼ぶ．上の手順により相手が秘密鍵を知っていることが分かるため，通信相手の特定への応用が可能である．

そこで，第３図に示すように，公開鍵暗号方式を２段階にわたって使用することにより，本システムの認証を行う．以下の方式では，認証局(以下ＣＡ)，通信を行う２つの無線ＬＡＮ装置Ａ，Ｂがそれぞれ，公開鍵と秘密鍵の組を所持している(ＳＫ$_{CA}$，ＰＫ$_{CA}$，ＣＫ$_{A}$，ＰＫ$_{A}$，ＣＫ$_{B}$，ＰＫ$_{B}$とする)．通信相手が，公開鍵ＰＫ$_{A}$，ＰＫ$_{B}$と対応する秘密鍵ＳＫ$_{A}$，ＳＫ$_{B}$を所持していることを検証することが最終的な目的である．

①通信に先だってＣＡの公開鍵ＰＫ$_{CA}$を無線ＬＡＮ装置に配布しておく．



第３図　端末認証の流れ

各無線ＬＡＮ装置は，ＣＡに秘密鍵ＳＫ$_{CA}$で自分の公開鍵ＰＫ$_{A}$，ＰＫ$_{B}$を暗号化してもらう(証明書の発行)．ＣＡは正しい情報にしか証明書を発行しないことが前提である．

②通信を行う無線ＬＡＮ装置は，互いに自分の公開鍵，ユーザ情報の証明書を送付しあう．

③受信した証明書を検証する．公開鍵ＰＫ$_{A}$，ＰＫ$_{B}$がＣＡによって署名されていることが分かる．

④乱数など，事前に予測しえないデータＪ$_{A}$，Ｊ$_{B}$を通信相手に送付しあう．

⑤Ｊ$_{A}$，Ｊ$_{B}$を秘密鍵ＳＫ$_{A}$，ＳＫ$_{B}$で署名して(Ｅ(ＳＫ$_{A}$，Ｊ$_{A}$)，Ｅ(ＳＫ$_{B}$，Ｊ$_{B}$)の生成)通信相手に送り返す．

⑥送られてきた署名(Ｅ(ＳＫ$_{A}$，Ｊ$_{A}$)，Ｅ(ＳＫ$_{B}$，Ｊ$_{B}$))を，その前に送られてきた通信相手の公開鍵ＰＫ$_{A}$，ＰＫ$_{B}$で検証(Ｆ(ＰＫ$_{B}$，Ｅ(ＳＫ$_{B}$，Ｊ$_{B}$))，Ｆ(ＰＫ$_{B}$，Ｅ(ＳＫ$_{B}$，Ｊ$_{B}$))の算出)する．通信相手がＣＡが署名した証明書に記載されている公開鍵ＰＫ$_{A}$，ＰＫ$_{B}$と対応する秘密鍵ＳＫ$_{A}$，ＳＫ$_{B}$を所持していることがわかる．公開鍵ＰＫと秘密鍵ＳＫの組を同時に生成することは容易であるが，公開鍵ＰＫに対応する秘密鍵ＳＫを後から生成することは困難である．したがって，単にＰＫ$_{A}$，ＰＫ$_{B}$とＳＫ$_{A}$，ＳＫ$_{B}$の対応を検証するだけでは不充分であるが，ＣＡによって署名された公開鍵と対応する秘密鍵を持っていることまで検証できれば，正しい秘密鍵を持った装置であることが確認できる．

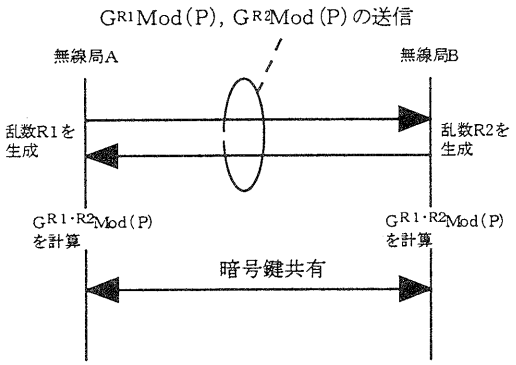
実際の手順においては，無線ＬＡＮ装置のユーザ情報(氏名，所属組織名など)も含んだ証明書をもちいることにより，特定の組織に所属するユーザだけに接続を許可する認証を行っている．

3－1－2．公開鍵配送

通信の暗号化において一般に広く用いられているのは，ＦＥＡＬ，ＤＥＳなどの，暗号化と復号に同一の鍵を用いる共通鍵暗号方式である．共通鍵暗号方式は，公開鍵暗号方式と比較して処理速度が速いという特徴を有するが，通信を行う両者は，暗号化／復号鍵を共有している必要がある．

暗号化／復号鍵を盗聴者に知られてしまうと，通信の内容を全て解読されてしまうため，通信を行う両者だけが秘密の暗号化／復号鍵を共有できる方法が必要である．その様な方法の中で，事前に秘密情報を共有している必要がなく，初対面の相手とも秘密の暗号

化／復号鍵を共有できるのが公開鍵配送方式である．



第４図　公開鍵配送の流れ

第４図に示すように，最も有名な Diffie-Hellman 公開鍵配送では，事前に通信を行う両者が，公開の暗号化／復号鍵生成用情報(G，P)を共有している．

①通信を行う両者は，各自が生成した乱数Ｒ１，Ｒ２を，上記の公開情報を元にG^{R1}Ｍｏｄ(P)，G^{R2}Ｍｏｄ(P)を計算して相手に送信する．

②受信すると，受信したデータを元に，$G^{R1\cdot R2}$Ｍｏｄ(P)を計算する．これは，Ｒ１，Ｒ２のいずれかを知らないと算出が困難な値であると考えられている．Ｒ１，Ｒ２自体は，通信路に送出されないので，盗聴者はこれらの値を知ることはできない．同様の方法として楕円 Diffie-Hellman 方式というアルゴリズムも考えられている．

次節に述べるように無線ＬＡＮによる mobile computing において公開鍵配送は，以下の２つの利点を持つ。

①事前に秘密情報を共有する必要も秘密情報を蓄積するデータベースにアクセスする必要もない

②乱数を両者が生成して送り合い，鍵を生成する方式であり，片方が暗号化／復号鍵を決めることができない

２つの利点を持つ．

３－２．本システムの認証手順の利点

本システムにおいて公開鍵認証，公開鍵配送を採用している理由は次の３つである．

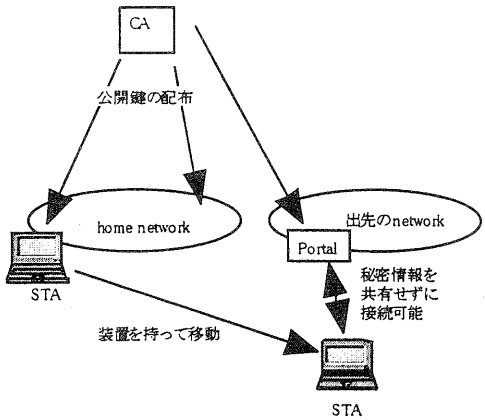
①認証・暗号鍵の事前共有のための設定が不必要である．

②相互認証を行うことができる

③秘密の認証情報の集中管理・制御の必要がない．

以下に，それぞれの利点について，mobile computing における重要性と公開鍵認証，公開鍵配送による実現方法を述べる．

①認証・暗号鍵の事前共有のための設定が不必要である．



第５図　公開鍵認証による出先のネットワークとの接続

前章で述べたとおり，広くインターネットを動き回るユーザがネットワークとの接続を行うためには，認証・暗号鍵の事前共有が必要な認証方法では不適である．３－１に述べたように，公開鍵認証，公開鍵配送を用いた接続手順では，事前にはＣＡの公開鍵など，広く公開された情報の共有以外は必要ない．このために，無線ＬＡＮ装置毎の認証情報を事前に設定しておかなくても，装置の認証，暗号化鍵の共有が可能である．

②相互認証を行うことができる

ＩＥＥＥ８０２．１１規格では，「親機」に相当するＰｏｒｔａｌと，子機に相当するＳＴＡの機能，動作は，ほぼ同等である．したがって，親機への「なりすまし」の危険性も，子機への「なりすまし」と同程度であると考えられる．したがって相互に認証を行う必要がある．

有線のネットワークへのアクセスポイント自体の正当性を検証する必要があることから，認証情報データベースにアクセスする認証手順は採用できない．

公開鍵認証・公開鍵配送を用いた手順は

(ａ)データベースにアクセスする必要がない

(ｂ)通信を行う無線局の一方が暗号鍵を決めて他方に通知する方式ではなく，乱数を両者が生成して送り合い，鍵を生成する方式である

ことから，相互認証に適した方式である．

③秘密の認証情報の集中管理・制御の必要がない

無線ＬＡＮによるモバイルコンピューティングに

おいては，次の３つの理由から，秘密の認証情報の集中管理・制御は困難である．

(a)相互認証を行う必要があるため，データベースへのアクセスを必要とする手順は採用できない

この点は②においてすでに論じた．

(b)秘密の認証情報データベースを Firewall の内側に置くと，外部からのデータベースアクセスが困難になる．一方，秘密の認証情報データベースを Firewall の外側に置くのはセキュリティ上の問題がある．

(c)秘密の認証情報データベースを管理運営する主体をどこにするべきかという政策的な問題が発生する．

この点については詳しく述べる．Ｄｏｐａ，ＰＩＡＦＳなどと最も異なる点は，ネットワークの運営主体が多様なことである．第１図に示す無線ＬＡＮを用いたモバイルコンピューティング標準的なケースでは，伝送路に運用主体が異なる，無線ＬＡＮを接続する有線のＬＡＮ，接続先のネットワークとユーザの職場のネットワークを結ぶインターネットそして，職場のＬＡＮが含まれている．

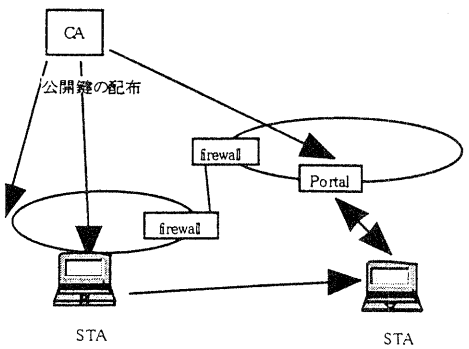
上記のように，無線ＬＡＮによるモバイルコンピューティングではネットワークが一体でないケースが想定されるため，認証，帰属などのアクセス制御においても集中管理の必要がないことが望ましい．

公開鍵認証では，ＣＡは以下の２つの理由から，ネットワーク上のどこに設置しても良い

- セッション開始時にＣＡにアクセスする必要がないこと
- ＣＡ自体には秘密の認証情報が蓄えられるわけではないこと．ＣＡは公開情報に対して電子署名するだけである．

ＣＡの設置形態として考えられるのは，以下の２つの場合である．

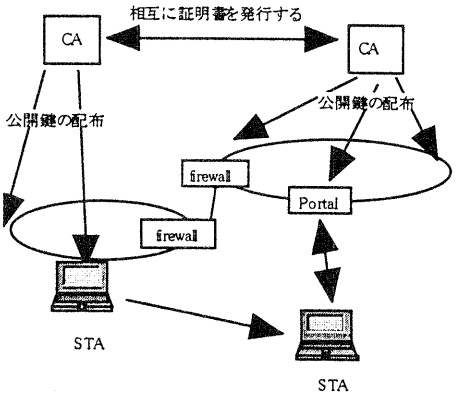
(1)第７図のように，Firewall の内側に



第６図　ＣＡの公開鍵を外部のネットワークにも配布す

ＣＡを設置する．無線端末は，直接ＣＡの管理者に証明書を発行してもらうか，Firewall の内側に在圏しているときにネットワークを経由して証明書の発行を受ける．Firewall の外側にあるＰｏｒｔａｌ，ＡＰに，ＣＡの公開鍵を配布しておけば，ＳＴＡとの証明書の交換，検証が行える．

(2)第７図のように，ＣＡはそれぞれのネットワークに存在し，相互に証明書(相手の公開鍵に対して)を発



行しあっている．

第７図　ＣＡが相互に証明書を発行する

各無線局は相互に

(a)自分の属するネットワークのＣＡが自局に対して発行した証明書

(b)通信相手の属するネットワークのＣＡが，自分の属するネットワークのＣＡに対して発行した証明書を送り合う．

(3)(a)と(b)を受信すると，(b)の検証をまず行い，通信相手の属するＣＡの公開鍵の正当性を確認する．次に，(a)を，通信相手の属するＣＡの公開鍵を用いて検証する．その後の手順は，３－１に述べたとおりである．

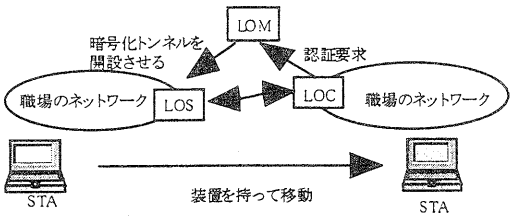
以上のいずれの場合においても，ＣＡを管理運営する団体をどこにするかなどの政治的・制度的な問題は発生しない．

４．ＡＬＡＮ

本システムは，ＮＴＴが開発したバーチャルＬＡＮシステム，ロジカルオフィス[9]に対応している．バーチャルＬＡＮと組み合わせることで，無線ＬＡＮ端末を持って，外部のネットワークに移動したユーザがマルチキャスト等のあらゆるレイヤ３プロトコルを用いたアプリケーションを，設定を変えずに使用するこ

とが出来る利点がある．

ロジカルオフィスは，第８図に示す構成で，以下のサービスの提供を行う．



第８図　ロジカルオフィス

(1)　ホームネットワークの外部にある端末は出先のネットワークでデータパケットを送信する．

(2) ネットワーク上を流れるデータパケットをキャプチャしたＬＯＣ(Logical Office Client)はＬＯＭ(Logical Office Management Server)に認証問い合わせを行う

(3) ＬＯＭは端末のホームネットワークのＬＯＳ(Logical Office Server)とＬＯＣの間にＩＰカプセリングのトンネルを開設させる

(4) ホームネットワークのイーサパケットはＬＯＣのＩＰアドレス宛に転送される

(5) ＬＯＣでＩＰカプセリングを解かれて，イーサパケットになり，端末に転送される

しかし，着信系のアプリケーションを，ホームネットワークに在圏しているときと同じ設定で使用するため，出先のネットワークに接続するＳＴＡが，自分の職場におけるＩＰアドレス，ＭＡＣアドレスを使い続けると，出先のネットワークにとってはネットワークアドレスが異なるＳＴＡが混在することになる．これがサブネット違反であり，ＳＴＡ宛のパケットは正常に転送されなくなるケースがあった．この問題を解決するため，ロジカルオフィスでは，移動 STA を収容する専用ネットワークを設ける．一方，本システムではミドルウェアとして，レイヤ２とレイヤ３の間にＡＬＡＮ層を設けている(第９図参照)．以下の手順をとることにより，ユーザは意識することなく，出先のネットワークから職場のネットワークへの接続がおこなえる．下記のＬＯＣ←→ＳＴＡのスクランブルがかかっている区間がＡＬＡＮ層である[2]．

(1)ＳＴＡは出先のネットワークのＬＯＣにアクセスする

(2) ＬＯＣはＬＯＭに認証問い合わせを行う

(3) ＬＯＭはＬＯＣにＳＴＡの属しているＣＵＧ(Closed User Group)のスクランブルパターンを通知する

(4) ＬＯＭはＳＴＡが属しているCUGのＬＯＳとＬＯＣの間にＩＰカプセリングのトンネルを開設させる

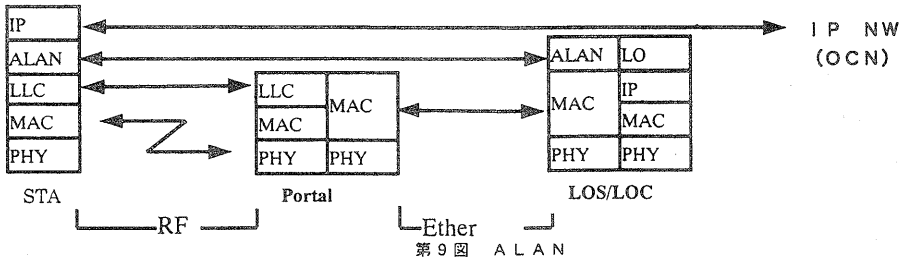
(5) CUG のイーサパケットはＬＯＣのＩＰアドレス宛に転送される

(6) ＬＯＣでＩＰカプセリングを解かれて，イーサパケットになる

(7) ＬＯＣ←→ＳＴＡ間は，イーサパケットのヘッダ中のタイプ値及びユーザデータに上記のスクランブルパターンを用いてスクランブルをかける．タイプ値にスクランブルがかかっているために，出先のネットワークの各ノードは，受信パケットを上位レイヤに受け渡さず，単に転送する．このためサブネット違反が起きない．ユーザデータにまでスクランブルをかけるのは，セキュリティ対策の一環である．

(8) ＳＴＡは転送されてきたパケットをディスクランブルして，ユーザデータを取り出す．

以上の流れとなる．この手順によって，ユーザが出先のネットワークにおいても，職場と変わらない環境で情報提供サービスを受けることが可能となる．



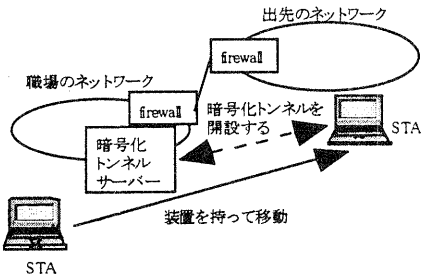
第９図　ＡＬＡＮ

5．本システムの今後の応用

本システムは，公開鍵認証のためにＣＡを用いているため，以下のような柔軟・多様な認証条件の設定を必要とするシステムを安価に構築できる．

5－1　ファイヤーウォール対策

本システムの使用者は，DOPA，PIAFS のユーザよりも，自分の office に接続して使用する指向が強いと予想される．本システムの高速伝送に対する需要は，自分の office と同じ環境で作業する必要から生じると考えられる．一方，ネットワーク外部からのアクセスに対しては，不法侵入者を排除するために firewall が設置されるのが一般的である．したがって，不法侵入者を排除しつつ，正規のユーザのアクセスを許可する仕組みを提供することが必要である．



第１０図　ＶＰＮ技術

正規ユーザだけ外部からのアクセスを許可するには，第１０図に示すように暗号化トンネルサーバーにおいて認証を行い，許可された端末のパケットだけ firewall を通りぬけるよう，暗号化トンネルサーバーと STA の間で暗号化トンネルを設定するＶＰＮ技術が普及している．本手順において本システムと同一の仕様のＣＡを用いた公開鍵認証方式を採用し，実際にサービス提供されている secure firewall システムがある．同一のＣＡを採用していることから，本システムを用いたモバイル環境を安価に構築することができる．

5－2．会議室での利用について

オフィスビルには，異なる企業同士の打ち合わせを行う会議室スペースが設けられているのが一般的である．本システムを用いて会議室スペースから職場のネットワークにアクセスする場合，セキュリティ上次の点が問題となる．

5－2－1．職場のネットワークに設定された firewall

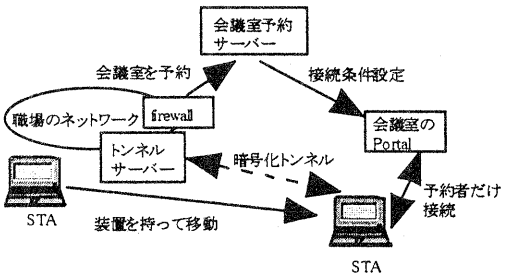
会議室は，社内の異なる組織に所属する社員によって使用される．社内のアクセスに対しても firewall を設けてセキュリティ対策を講じるのが一般的であるため，会議室から，利用者の所属するネットワークの firewall を通りぬけてアクセスできる機能が必要がある．

5－2－2．会議室のアクセスポイントの接続条件

上と同様に，会議室のアクセスポイントは，利用されている時間のみ，予定されている利用者のみ接続を許可できる機能が必要である．

5－2－3．実現方法

上記の会議室からのアクセスシステムの実現は，５－１を用いた secure firewall　と，会議室予約システムを以下のように組み合わせることにより可能である(第１１図)．



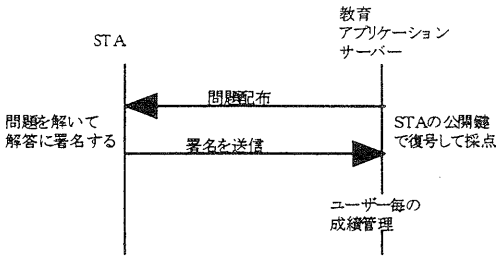
第１１図　会議室における本システム利用

(1)会議室予約システムは，社員からの会議室予約を受け付けると，遠隔から会議室のアクセスポイントの接続条件の設定を行う．
(2)予約した社員は，会議室のアクセスポイントから Secure firewall を用いて自分の職場のネットワークにアクセスする．

6－2．教育用利用について

教室の外の環境でも(学校の図書室など)でも学習が行える自習用アプリケーションの開発が行われているが，ネットワークと組み合わせた場合，以下のような利用が考えられる．(第１２図)
(1)教育用アプリケーションサーバー
(以下ＥＡＳ；Education Application Server)がユーザ

に問題を配布する.
(2)ユーザは問題を解く
(3)ユーザは自分の解答を秘密鍵で署名して，自分の公開鍵の証明書(3章を参照)と一緒に，ＥＡＳに送信する
(4)ＥＡＳは，ユーザから送られてきた署名を，証明書に記載された公開鍵で復号し，採点する．ユーザ単位で成績の管理などを行う．



第１２図　本システムの教育用利用

上記において，(1)では本システムの位置管理機能を用いて問題の配布が実現され，(3)以下では，公開鍵認証機能を用いて特定のユーザから送られてきた答案の採点が実現されている．

本アプリケーションにおいて，公開鍵認証を採用する利点は，同一の秘密鍵／公開鍵のペアを用いて，複数のサーバーにアクセスして上記と同様のサービスの提供を受けることが可能な点である．ユーザは公開鍵を複数のサーバーに報知することにより，プライバシー確保，ユーザ単位の管理を必要とする多様なサービスの提供を受けることができる．同一の秘密鍵／公開鍵のペアを使用できるため，秘密情報管理が簡易である．

本アプリケーションにおいても，本システムと同一のＣＡを採用することにより，システム構築にかかる費用が安価になる．

６．まとめ

本システムの mobile computing に対する利点と，今後予想される利用形態について述べてきた．バーチャル
ＬＡＮ機能と公開鍵認証機能を無線ＬＡＮに付加することにより，従来の無線ＬＡＮの利用範囲を飛躍的に拡大することができる．

1) 谷本，針生，磯田，中島，“ロジカルオフィスサービス “，NTT R&D，Vol.45, No.10, 1996.

2) 森田，友田，大畑，増井，“2.4GHz 帯無線 LAN と組み合わせた移動型 LAN システム-モバイル LAN システム開発-”，1997 年信学総大，B-5-275，1997.